Email Use Policy

Purpose

This policy establishes standards for the proper use of DC government-provided electronic mail (email) services.

Scope

This policy applies to:

- All electronic mail systems and services provided or owned by the DC Government.
- Transactional information associated with email records (such as email headers, summaries, addresses, and addressees) as well as the contents of those records.
- All users of DC Government email services, including:
    - Full and part-time employees
    - Contractors authorized to use DC Government-owned equipment or network resources
    - Volunteers who have been provided with an email account/service and
    - All other users of DC Government information technology resources.
    - All DC Government email records in the possession of any DC Government email users.

Policy Details

Introduction

Email is an efficient and timely communications tool that is provided by the DC Government to its employees, contractors, and volunteers to assist them in supporting DC government functions and conducting the government's business within its own organization, with government and private business partners, and with the public. Appropriate use of the DC Government email system can enhance productivity and intra-governmental communication, but inappropriate use can conflict with DC government policies and compromise availability of the system for all. This policy defines requirements and prohibitions for appropriate use of the DC government email system or any messaging system that uses the District's computer network.

Principles

- Use of the DC government email system constitutes consent to abide by all elements of this policy, including such reviews of email correspondence as may be necessary and appropriate to effect DC Government policies concerning the use of the email system and in aid of law-enforcement and auditing activities of federal and District of Columbia government agencies.
- DC Government email systems and services are "DC Government facilities" as that term is used in other policies and guidelines. Any electronic mail address or account assigned by the DC Government to individuals, sub-units, or functions of the DC Government is the property of the District of Columbia and under management control of the Office of the Chief Technology Officer.

- All DC government policies relating to intellectual property protection, privacy, misuse of government resources, sexual harassment, data security, and confidentiality apply to use of DC Government email by persons and entities described under "Scope," above.
- Emails are the equivalent of letters sent on official letterhead, and must therefore be written in a professional and courteous tone.
- DC government email is public, not private communication, not only because its principal purpose is the conduct of DC government functions, but also because the email system permits forwarding and other wide distribution of messages without the consent of the sender. Therefore, senders and receivers of email can have no expectation of privacy with respect to DC government email messages.
- Email messages are public records and are therefore subject to public inspection, FOIA requests, and legal discovery, unless otherwise protected by DC or federal law.

Allowable Uses

- Communication and information exchange directly related to the mission, charter, or work tasks of a DC government agency
- Research and information exchange in support of standards, analysis, advisory, and professional development activities related to the user's DC government duties
- Announcement of DC government laws, procedures, policies, rules, services, programs, information, or activities, subject to the broadcast email requirements described below
- Application for, or administration of, contracts or grants for DC government programs or research
- Other governmental administrative communications not requiring a high level of security
- Interagency and external broadcast correspondence that:
    - Is limited to 100 recipients or fewer,
    - Is not sent to the group distribution list of any other agency, and
    - Does not constitute or contain (as an attachment or otherwise) any inter-agency or external bulletin, newsletter, announcement, promotional material, manual, guide, brochure, or marketing collateral, all of which must be posted on websites and not sent in group emails outside the sender's agency list.
- Interagency and external broadcast emails with distribution greater than 100 recipients that are authorized in advance by the Director of Communications of the Executive Office of the Mayor (EOM) or the Chief Technology Officer
- Mayoral broadcast missives, upon 2 hours' notice to OCTO or with shorter notice to OCTO, in the discretion of the Director of Communications, EOM
- Incidental personal purposes, provided that such use does not:
    - Directly or indirectly interfere with the DC Government operation of computing facilities or electronic mail services,
    - Burden the DC Government with noticeable incremental cost, or
    - Interfere with the email user's employment or other obligations to the DC Government.

Prohibited Uses

- Any purpose that violates a federal or DC government law, code or policy, standard or procedure
- The advertising or other promotion of any private business enterprise or activity
- Transmission or solicitation of information or statements that contain profane language, pander to bigotry, sexism, or other forms of prohibited discrimination, or can in any way be construed as intending to harass or threaten another individual, sexually or otherwise
- Any activity with religious or political purposes outside the scope of the user's assigned and authorized governmental duties
- Any unauthorized purchase

- Sending email under names or addresses other than the employee's own officially designated DC government email address
- Adding, removing, or modifying identifying network header information ("spoofing") in an effort to deceive or mislead recipients
- Opening any "executable" email attachments (e.g., .exe, .bat, .scr, .vbs) from any source
- Sending or forwarding "chain" letters, i.e., those that ask the receiver to forward the message to multiple recipients
- Sending any attachment files larger than 10 megabytes (MB)
- Sharing organized District email lists with any person outside the District, except as required by the Freedom of Information Act, subpoena, or other compulsory process
- Setting email correspondence to forward automatically to an outside (non-District) address
- "Broadcast" emails that do not meet the "broadcast" email requirements above
- Disruption, obstruction, or burden of network resources
- Unauthorized enhancements or add-on software to Outlook (e.g., animations, backgrounds, pictures)
- Use of non-District email services such as Yahoo or AOL on the District's computer network
- The intentional or negligent introduction of computer viruses into any DC Government systems; agencies must prevent the introduction of computer viruses into DC government systems and must install District-standard virus-scanning software to check any software downloaded as email attachments.
- Transmission of sensitive (e.g., confidential) information unless protected by an approved encryption mode and/or identified as shown below
    - Sensitive information includes medical information, information covered by attorney-client privilege, information subject to the Privacy Act, proprietary information, or other information which must be protected from unauthorized disclosure.
    - Sensitive (e.g., confidential) messages must be clearly identified immediately below the message header (i.e., the Subject, Data, From, and To lines) as "SENSITIVE/CONFIDENTIAL INFORMATION [or ATTORNEY/CLIENT PRIVILEGED INFORMATION] - DO NOT RELEASE TO UNAUTHORIZED PERSONNEL." In such cases, the sender must also be certain that the recipient is properly authorized to receive and view the information.
    - For approved encryption modes, refer to applicable information security policies, standards, and procedures.

Sanctions

Violations of District email policy will result in:

- Upon notice to the violator, disabling of his/her email account for a period of time consistent with the seriousness of the violation, unless a written request for reinstatement is submitted by the agency Director/designate to the OCTO Director of IT Security.
- Where an email account is found to be broadcasting a virus or otherwise placing the email system in jeopardy, disabling the account without notice to the violator, with reinstatement as described above
- Other corrective action in the discretion of the violator's agency Director

Statutory Authority

DC Official Code § 1-1403.

Roles and Responsibilities

All DC Government Email Users

- Users of DC email must use the service only for the Allowable Uses defined above and refrain from any of the Prohibited Uses defined above.
- Users must change passwords with regular frequency, in accordance with applicable agency and OCTO standards and recommendations.

DC Government Agencies

- Each agency is responsible for its employees' and contractors' compliance with this policy and is expected to familiarize each user with this policy.
- Because transmission of email may involve routing over an unsecured network, it is the responsibility of each agency to protect sensitive (i.e., confidential) information from intentional, inappropriate, or accidental disclosure, and to protect the DC government and individual users from loss or harm.
- Agencies are responsible for the investigation of alleged or suspected violations of this policy, and the referral of violations to OCTO for suspension of service to users.
- Agencies are responsible for identifying those email records within their users' accounts that are to be treated as "permanently valuable" for retention purposes (see "OCTO," below).

OCTO

- The OCTO Director of IT Security must develop and update email security policy and maintain awareness of email-related threats, vulnerabilities, and security issues.
- The Director of IT Security will maintain a content filtering system which scans the contents of messages on the DC Government email system, rejects messages containing content that may violate this policy, and issue the sender a notification advising that the message has been rejected, and why, so that the message can be corrected and resent.
- However, neither OCTO nor any agency or instrumentality of the DC Government undertakes to protect users from receiving electronic mail they may find offensive, or to guarantee that electronic mail received was in fact sent by the purported sender.
- OCTO will maintain "permanently valuable records" in the DC Government email system in a manner and according to a schedule to be established by the Executive Office of the Mayor. Each agency is responsible for identifying those email records within their users' accounts that are to be treated as "permanently valuable." Emails and attachments not identified as "permanently valuable" will be archived electronically six months after creation and deleted permanently from the DC Government email system one year after creation.
- Because email is public, not private communication, OCTO may monitor any or all DC Government email traffic to determine compliance with this and related policies.

DISCLAIMER OF LEGAL RIGHTS

Nothing in this statement of policy shall be deemed to create any legal right on the part of a user of the email system, nor any legal obligation on the part of OCTO or any person having authorized access to search or review email correspondence in the system.